CLAIMS

What is claimed is:

1. An optical data storage medium comprising:

optically-readable material suitable for storing data therein; and

stored within said optically-readable material, instructional data for an optical media content protection scheme, said instructional data being configured to cause logic associated with an optical media receiving device to operatively perform in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium.

2. The optical data storage medium as recited in Claim 1, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

3. The optical data storage medium as recited in Claim 2, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

4. The optical data storage medium as recited in Claim 1, further comprising at least one type of additional data stored within said optically-readable material, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said

optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

5. The optical data storage medium as recited in Claim 1, further comprising:

at least one optically-detectable authentication feature.

6. The optical data storage medium as recited in Claim 5, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

7. The optical data storage medium as recited in Claim 6, wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material.

8. The optical data storage medium as recited in Claim 6, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

9. The optical data storage medium as recited in Claim 8, further comprising:

COA information data stored within said optically-readable material.

10. The optical data storage medium as recited in Claim 9, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

11. The optical data storage medium as recited in Claim 5, further comprising:

at least one top surface material and wherein at least one of the following occurs:

said at least one optically-detectable authentication feature is formed on said top surface material;

said at least one optically-detectable authentication feature is formed below said top surface material; and

said at least one optically-detectable authentication feature extends at least partially into said top surface material.

12. An optical data storage medium comprising:

optically-readable material suitable for storing data therein; and

at least one optically-detectable non-data-based, physical authentication feature having a substantially unique pattern and comprising at least one optically detectable material.

13. The optical data storage medium as recited in Claim 12, wherein said optically detectable material includes at least one material selected from a

group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material.

14. The optical data storage medium as recited in Claim 12, wherein said authentication feature forms an optically-detectable certificate of authentication (COA).

15. The optical data storage medium as recited in Claim 14, further comprising:

COA information data stored within said optically-readable material.

16. The optical data storage medium as recited in Claim 15, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

17. The optical data storage medium as recited in Claim 12, further comprising at least one top surface material, and wherein at least one of the following statements is true:

said authentication feature is formed on said top surface material;

said authentication feature is formed below said top surface material; and

said authentication feature is formed so as to extend at least partially into said top surface material.

18. An apparatus comprising:

means for storing instructional data for an optical media content protection scheme within an optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium.

19. The apparatus as recited in Claim 18, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

20. The apparatus as recited in Claim 19, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

21. The apparatus as recited in Claim 18, further comprising:

means for storing at least one type of additional data within said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

22. The apparatus as recited in Claim 18, further comprising:

means for causing at least one optically-detectable authentication feature to be included in said optical data storage medium.

23. The apparatus as recited in Claim 22, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

24. The apparatus as recited in Claim 23, wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material.

25. The apparatus as recited in Claim 23, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

26. The apparatus as recited in Claim 25, further comprising:

means for storing COA information data within said optical data storage medium.

27. The apparatus as recited in Claim 26, wherein said COA information data includes at least one type of data associated with said COA selected from a

group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

28. The apparatus as recited in Claim 27, further comprising:

means for generating said COA information data.

29. The apparatus as recited in Claim 22, further comprising:

wherein said optical data storage medium includes at least one top surface material, and further comprising at least one means for causing at least one of the following functions to occur:

forming said at least one optically-detectable authentication feature on said top surface material;

forming at least one optically-detectable authentication feature below said top surface material; and

forming said at least one optically-detectable authentication feature such that said optically-detectable authentication feature extends at least partially into said top surface material.

30. An apparatus comprising:

means for forming at least one optically-detectable non-data-based, physical authentication feature as part of an optical data storage medium, said authentication feature having a substantially unique pattern and comprising at least one optically detectable material.

31. The apparatus as recited in Claim 30, wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material.

32. The apparatus as recited in Claim 30, wherein said authentication feature is an optically-detectable certificate of authentication (COA).

33. The apparatus as recited in Claim 32, further comprising:

means for storing COA information data within said optical data storage medium.

34. The apparatus as recited in Claim 33, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

35. The apparatus as recited in Claim 30, wherein said optical data storage medium includes at least one top surface material, and further comprising at least one means for causing at least one of the following functions to occur:

forming said at least one optically-detectable authentication feature on said top surface material;

forming at least one optically-detectable authentication feature below said top surface material; and

forming said at least one optically-detectable authentication feature such that said optically-detectable authentication feature extends at least partially into said top surface material.

36. An apparatus comprising:

a data storage device configurable to write data to an optical data storage medium; and

logic operatively coupled to said configured to said data storage device and configured to cause said data storage device to record instructional data for an optical media content protection scheme within said optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content on said an optical data storage medium.

37. The apparatus as recited in Claim 36, wherein said optical media content protection scheme includes digital rights management (DRM) protection scheme.

38. The apparatus as recited in Claim 37, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

39. The apparatus as recited in Claim 36, wherein said logic is further configured to cause said data storage device to record at least one type of additional data within said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and content data.

40. The apparatus as recited in Claim 36, wherein said optical data storage medium further includes at least one optically-detectable authentication feature.

41. The apparatus as recited in Claim 40, wherein said data storage device is further configurable to detect said at least one optically-detectable authentication feature and provide resulting authentication feature information to said logic.

42. The apparatus as recited in Claim 40, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

43. The apparatus as recited in Claim 41, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

44. The apparatus as recited in Claim 43, wherein said logic is further configured to cause said data storage device to record COA information data within said optical data storage medium.

45. The apparatus as recited in Claim 44, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

46. An apparatus comprising:

an authentication feature forming mechanism configured to apply authentication feature forming material to an optical data storage medium so as to form at least one optically-detectable non-data-based, physical authentication feature as part of said optical data storage medium, said authentication feature having a substantially unique pattern and comprising at least one optically detectable material.

47. The apparatus as recited in Claim 46, wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material.

48. The apparatus as recited in Claim 46, wherein said authentication feature is an optically-detectable certificate of authentication (COA).

49. A method comprising:

storing instructional data for an optical media content protection scheme within an optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium.

50. The method as recited in Claim 49, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

51. The method as recited in Claim 50, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

52. The method as recited in Claim 49, further comprising:

storing at least one type of additional data within said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

53. The method as recited in Claim 49, further comprising:

causing at least one optically-detectable authentication feature to be included in said optical data storage medium.

54. The method as recited in Claim 53, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

55. The method as recited in Claim 54, wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material.

56. The method as recited in Claim 54, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

57. The method as recited in Claim 56, further comprising:

storing COA information data within said optical data storage medium.

58. The method as recited in Claim 57, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

59. The method as recited in Claim 58, further comprising:

generating said COA information data.

60. The method as recited in Claim 53, further comprising:

wherein said optical data storage medium includes at least one top surface material, causing at least one of the following acts to occur:

forming said at least one optically-detectable authentication feature on said top surface material;

forming at least one optically-detectable authentication feature below said top surface material; and

forming said at least one optically-detectable authentication feature such that said optically-detectable authentication feature extends at least partially into said top surface material.

61. A method comprising:

forming at least one optically-detectable non-data-based, physical authentication feature as part of an optical data storage medium, said authentication feature having a substantially unique pattern and comprising at least one optically detectable material.

62. The method as recited in Claim 61, wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material.

63. The method as recited in Claim 61, wherein said authentication feature is an optically-detectable certificate of authentication (COA).

64. The method as recited in Claim 63, further comprising:

storing COA information data within said optical data storage medium.

65. The method as recited in Claim 64, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

66. The method as recited in Claim 61, wherein said optical data storage medium includes at least one top surface material, the method further comprising causing at least one of the following acts to occur:

forming said at least one optically-detectable authentication feature on said top surface material;

forming at least one optically-detectable authentication feature below said top surface material; and

forming said at least one optically-detectable authentication feature such that said optically-detectable authentication feature extends at least partially into said top surface material.

67. A computer-readable medium comprising computer-implementable instructions for causing at least one processor to perform acts comprising:

writing instructional data for an optical media content protection scheme to an optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium.

68. The computer-readable medium as recited in Claim 67, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

69. The computer-readable medium as recited in Claim 68, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

70. The computer-readable medium as recited in Claim 67, further comprising:

writing at least one type of additional data to said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

71. The computer-readable medium as recited in Claim 67, wherein said optical data storage medium further includes at least one optically-detectable authentication feature.

72. The computer-readable medium as recited in Claim 71, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA) and further comprising:

writing COA information data to said optical data storage medium.

73. The computer-readable medium as recited in Claim 72, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

74. The computer-readable medium as recited in Claim 71, further comprising:

generating said COA information data.

75. An apparatus comprising:

non-volatile memory;

an interface mechanism suitable for receiving a removable optical data storage medium, accessing instructional data associated with an optical media content protection scheme from said optical data storage medium, and outputting said accessed instructional data;

logic operatively coupled to said interface mechanism and said non-volatile memory and configured to receive said accessed instructional data and in response thereto update a current optical media content protection scheme stored in said non-volatile memory and thereafter while accessing associated content data stored on said optical data storage medium operatively adhere to said updated current optical media content protection scheme.

76. The apparatus as recited in Claim 75, wherein said current optical media content protection scheme causes said logic to adhere to a digital rights management (DRM) protection scheme.

77. The apparatus as recited in Claim 76, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

78. The apparatus as recited in Claim 75, wherein said interface mechanism is further configured to access and output to said logic at least one type of additional data stored on said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

79. The apparatus as recited in Claim 75, wherein said interface mechanism is further configured to detect at least one optically-detectable authentication feature that is part of said optical data storage medium and output corresponding information to said logic.

80. The apparatus as recited in Claim 79, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

81. The apparatus as recited in Claim 80, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

82. The apparatus as recited in Claim 81, wherein said interface mechanism is further configured to access COA information data stored within said optical data storage medium and provide said COA information data to said logic.

83. The apparatus as recited in Claim 82, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

84. The apparatus as recited in Claim 82, wherein said logic is further configured to verify said COA information data, and is configured to update said current optical media content protection scheme stored in said non-volatile memory once said COA information data has been verified.

85. The apparatus as recited in Claim 84, wherein said interface mechanism is further configured to access license information data stored within said optical data storage medium and provide said license information data to said logic, and wherein said logic is configured to verify said license information data to determine if content data stored on said optical data storage medium can be accessed.

86. The apparatus as recited in Claim 85, wherein said logic maintains license usage information within said non-volatile memory.

87. An apparatus comprising:

an interface mechanism suitable for receiving a removable optical data storage medium, accessing and outputting data stored thereon, and detecting at least one optically-detectable authentication feature that is part of said optical data storage medium and outputting corresponding authentication feature information;

logic operatively coupled to said interface mechanism and configured to receive said accessed data and said authentication feature information and in response thereto determine if content data stored on said optical data storage medium can be accessed.

88. The apparatus as recited in Claim 87, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

89. The apparatus as recited in Claim 88, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

90. The apparatus as recited in Claim 89, wherein accessed data includes COA information data having at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

91. A method comprising:

reading instructional data associated with an optical media content protection scheme from an optical data storage medium;

updating a current optical media content protection scheme based on said instructional data; and

based on said updated current optical media content protection scheme, determining if a valid license exists prior to accessing associated content data stored on said optical data storage medium.

92. The method as recited in Claim 91, wherein said current optical media content protection scheme implements a digital rights management (DRM) protection scheme.

93. The method as recited in Claim 92, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

94. The method as recited in Claim 93, further comprising accessing at least one type of additional data stored on said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

95. The method as recited in Claim 91, further comprising detecting at least one optically-detectable authentication feature that is part of said optical data storage medium.

96. The method as recited in Claim 95, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

97. The method as recited in Claim 96, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

98. The method as recited in Claim 97, further comprising reading COA information data from said optical data storage medium, said COA information data including at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.

99. The method as recited in Claim 98, further comprising verifying said COA information data, and updating said current optical media content protection scheme once said COA information data has been verified.

100. The method as recited in Claim 99, further comprising maintaining license usage information.

101. A method comprising:

receiving a removable optical data storage medium;

detecting at least one optically-detectable authentication feature that is part of said optical data storage medium;

outputting authentication feature information;

determining if content data stored on said optical data storage medium can be accessed based at least in part on said authentication feature information.

102. The method as recited in Claim 101, wherein said optically-detectable authentication feature includes a plurality of optically-detectable authentication features forming a substantially unique pattern using at least one optically detectable material.

103. The method as recited in Claim 102, wherein said plurality of optically-detectable authentication features form an optically-detectable certificate of authentication (COA).

104. The method as recited in Claim 101, further comprising:

reading COA information data from said optical data storage medium, said COA information data being associated with said COA and selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data.